Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;

delivering the plurality of encrypted sections to the customer processing platform; and

delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein delivering the plurality of decryption keys comprises:

delivering to the customer processing platform a current key of the plurality of decryption keys;

delivering to the customer processing platform a next key of the plurality of decryption keys; and

causing the current key to be destroyed at the customer processing platform only after at least the next key of the plurality of decryption keys has been received.

2. (Cancelled)

3. (Cancelled)

4. (Currently Amended) The method of claim ~~3~~1, wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections to be subsequently processed.

5. (Currently Amended) The method of claim ~~3~~1, wherein the current encrypted section is a first one of the plurality of encrypted sections, and wherein delivering to the customer processing platform a next key of the plurality of decryption keys and causing the current key to be destroyed at the customer processing platform are repeated for each of the plurality of encrypted sections following the first encrypted section.

6. (Currently Amended) The method of claim 1, wherein delivering to the customer processing platform a plurality of decryption keys comprises:

providing key control software to the customer processing platform, the key control software being adapted to:

receive [[a]]the current decryption key for [[one of]]the current encrypted section of the plurality of encrypted sections;

receive [[a]]the next decryption key for the next encrypted section of the plurality of encrypted sections;

complete decryption of the [[one]]current section;

begin decryption of the next section; and

destroy the current decryption key after decryption of the next section has begun.

7. (Original) The method of claim 1 further comprising:

billing a customer for delivery of the encrypted sections, and then billing the customer each time the data content is used at the customer processing platform.

8. (Original) The method of claim 1, wherein the data content is video content or music content, and wherein use of the data content at the customer processing platform comprises decryption and playback of the data content.

9. (Original) The method of claim 1, wherein each of the plurality of encryption keys comprises a respective symmetric cryptographic key, and wherein each of the plurality of decryption keys comprises the symmetric cryptographic key of its corresponding encryption key.

10. (Original) The method of claim 1, further comprising:

generating each of the plurality of encryption keys using an identifier associated with the customer processing platform, to thereby generate a plurality of customer processing platform-specific keys.

11. (Original) The method of claim 10, wherein generating comprises generating each of the plurality of customer processing platform-specific keys using the identifier and a respective key generation seed value.

12. (Original) The method of claim 11, wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the respective key generation seed values.

13. (Original) The method of claim 1, further comprising:

generating a respective transmission value for each of the plurality of encryption keys using an identifier associated with the customer processing platform,

wherein delivering to the customer processing platform a plurality of decryption keys comprises delivering the transmission values.

14. (Currently Amended) The method of claim 1, further comprising:

delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform via a peer-to-peer network; and

delivering the plurality of decryption keys from the data content provider to the second customer processing platform, wherein the decryption keys are delivered in a manner such that the second customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein the plurality of decryption keys are encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform.

15. (Original) A computer-readable medium storing instructions which, when executed by a processor at a data content provider, perform a method according to claim 1.

16. (Currently Amended) A method of receiving and controlling playback of data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of data content, each of which has been encrypted using a respective encryption key; and

for each encrypted section:

receiving a decryption key in respect of the encrypted section;

decrypting and playing back the encrypted section using the decryption key; and

destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section.

17. (Original) The method of claim 16, further comprising, for each encrypted section:

destroying decrypted data content at the customer processing platform after completing playback of the encrypted section.

18. (Original) The method of claim 16, wherein the communications medium is the public Internet.

19. (Original) The method of claim 16, wherein, for each encrypted section, the encryption key is the same as the decryption key.

20. (Currently Amended) The method of claim 16, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform via a peer-to-peer network, and wherein, for each encrypted section, the decryption key is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform.

21. (Original) A computer-readable medium storing instructions which, when executed by a customer processing platform, perform a method according to claim 16.

22. (Original) The method of claim 16, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform.

23. (Original) The method of claim 16, wherein receiving each decryption key comprises receiving a transmission value that is determined based on the decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section:

recovering the decryption key from the transmission value.

24.–33.(Cancelled)

34. (Currently Amended) A method for controlling use of encrypted data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device;

comparing the customer verification information with corresponding stored customer information ; and

where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer;

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted data content; and

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data; and

causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device.

35. (Currently Amended) A computer readable medium storing software code executable by a processing platform, the software code comprising:

first software code for coordinating downloading a plurality of sections of data content each encrypted with a respective one of a plurality of encryption keys to a customer computer system from a data content service provider system or another customer computer system; and

second software code for establishing a connection with the data content service provider system to obtain permission to use the data content, and for using the data content where permission is obtained from the data content service provider system by receiving a corresponding one of a plurality of decryption keys for each encrypted section of data content and decrypting the encrypted section using the corresponding one of the plurality of decryption keys such that the processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein for each encrypted section of data content the second software code destroys the received decryption key corresponding to the encrypted section of data content only after receiving at least the decryption key corresponding to the next encrypted section of data content.

36. (Original) The computer readable medium of claim 35, wherein the second software code obtains further permissions from the data content service provider system to continue using the data content.

37. (Cancelled)

38. (Currently Amended) A system for delivering data content from a data content provider to a customer processing platform and controlling use of the data content at the customer processing platform, comprising:

means for encrypting each of a plurality of sections of the data content using a respective one of a plurality of encryption keys to produce a corresponding plurality of encrypted sections;

means for delivering the plurality of encrypted sections to the customer processing platform; and

means for delivering to the customer processing platform a plurality of decryption keys corresponding to the plurality of encryption keys, wherein the decryption keys are delivered in a manner such that the customer processing platform has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein the means for delivering the plurality of decryption keys comprises:

means for delivering to the customer processing platform a current key of the plurality of decryption keys; and

means for delivering to the customer processing platform a next key of the plurality of decryption keys,

the customer processing platform comprising:

means for destroying the current key at the customer processing platform only after at least the next key of the plurality of decryption keys has been received.

39. (Currently Amended) The system of claim 38, wherein the customer processing platform comprises:

means for requesting the data content to be delivered to the customer processing platform via a peer-to-peer network connection;

means for receiving the plurality of encrypted sections via the peer-to-peer network connection;

means for receiving, for each encrypted section, the decryption key in respect of the encrypted section over an encrypted decryption key delivery channel; and

means for decrypting and playing back the encrypted section using the decryption key; ~~and~~, wherein

the means for destroying the current decryption key comprises means for destroying the current decryption key, after completing playback of the current encrypted section and beginning playback of the next encrypted section.

40. (Currently Amended) A data content distribution system comprising:

a data content server configured to receive download requests and permission requests for data content, to encrypt a plurality of sections of requested data content using respective encryption keys to thereby generate a plurality of encrypted sections and to transmit the encrypted sections of the data content in response to a received download request for the data content, and to transmit each of a plurality of decryption keys respectively corresponding to the encryption keys in response to a permission request for the data content; and

a data content download controller configured to generate download requests, to receive encrypted sections of data content in response to download requests, to generate permission requests when downloaded data content is to be used, and for each encrypted section of data content to be used, to receive a corresponding one of the plurality of decryption keys, and to decrypt the encrypted section using the corresponding one of the plurality of decryption keys; said data content server operable to transmit the plurality of decryption keys in a manner such

that the data content download controller has simultaneous possession of at most a subset of the plurality of decryption keys at any time, wherein, for each encrypted section, the data content download controller destroys the decryption key corresponding to the encrypted section only after at least the decryption key corresponding to the next encrypted section of the plurality of encrypted sections has been received.

41. (Original) The system of claim 40, comprising a data network connecting the data content server and the data content download controller.

42. (Original) The system of claim 41, further comprising a plurality of data content download controllers connected to the data network.

43. (Original) The system of claim 42, wherein each of the plurality of data content download controllers is implemented in conjunction with a respective customer computer system and is further configured to download encrypted sections of data content from other customer computer systems.

44. (New) The method of claim 1, wherein causing the current key to be destroyed at the customer processing platform comprises:

causing the current key to be destroyed at the customer processing platform after processing of the current encrypted section of the plurality of encrypted sections with the current key has been completed and processing of a next encrypted section of the plurality of encrypted sections with the next key has begun.

45. (New) The method of claim 1, wherein causing the current key to be destroyed at the customer processing platform comprises:

causing the current key to be destroyed at the customer processing platform before processing of the next encrypted section has been completed.

46. (New) The method of claim 1, wherein:

delivering to the customer processing platform a plurality of decryption keys comprises:

delivering the plurality of decryption keys to the customer processing platform over an encrypted decryption key delivery channel; and

delivering the plurality of encrypted sections to the customer processing platform comprises:

providing the plurality of encrypted sections to a peer-to-peer network, wherein the customer processing platform downloads the plurality of encrypted sections via the peer-to-peer network.

47. (New) The method of claim 34, wherein causing a key for a preceding portion of the encrypted data to be deleted comprises:

causing the key for the preceding portion of the encrypted data to be deleted from the customer data content processing device only after decryption of the subsequent portion of the encrypted data has begun.

48. (New) The computer readable medium of claim 35, wherein the second software code destroys the received decryption key corresponding to the encrypted section of data content only after decryption of the next encrypted section of data content has begun.

49. (New) The system of claim 38, wherein the means for causing the current key to be destroyed at the customer processing platform comprises:

means for causing the current key to be destroyed at the customer processing platform after processing of the current encrypted section of the plurality of encrypted sections with the current key has been completed and processing of a next encrypted section of the plurality of encrypted sections with the next key has begun.

50. (New) The system of claim 38, wherein the means for causing the current key to be destroyed at the customer processing platform comprises:

means for causing the current key to be destroyed at the customer processing platform before processing of the next encrypted section has been completed.

51. (New) The system of claim 38, wherein:

the means for delivering to the customer processing platform a plurality of decryption keys comprises:

means for delivering the plurality of decryption keys to the customer processing platform over an encrypted decryption key delivery channel; and

the means for delivering the plurality of encrypted sections to the customer processing platform comprises:

a peer-to-peer network, wherein the customer processing platform downloads the plurality of encrypted sections via the peer-to-peer network.

52. (New) The system of claim 40, wherein the data content download controller destroys the decryption key corresponding to the encrypted section only after decryption of the encrypted section has completed and decryption of the next encrypted section of the plurality of encrypted sections with the decryption key corresponding to the next encrypted section of the plurality of encrypted sections has begun.

53. (New) The system of claim 43, comprising an encrypted decryption key channel for delivery of the plurality of decryption keys, wherein the data network comprises a peer-to-peer network connecting the customer computer systems to share the encrypted sections of data content, and wherein the encrypted decryption key channel is separate from the peer-to-peer network.